

# Developer Report

**Acunetix Security Audit** 

2024-08-18

Generated by Acunetix

1

# Target - http://172.23.144.1/

### Scan details

Scan information	
Start url	http://172.23.144.1/dvwa/vulnerabilities
Host	http://172.23.144.1/

#### Threat level

### **Acunetix Threat Level 2**

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

#### Alerts distribution

Total alerts found	5
	0
A High	0
∧ Medium	3
∨ Low	0
(i) Informational	2

## **Alerts summary**

## ∧ Insecure HTTP Usage

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected items	Variation
Web Server	1

## Password transmitted over HTTP

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VIN/SI:N/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: Not Availability Impact to the Vulnerable System: Not Confidentiality Impact to the Subsequent System: Not Integrity Impact to the Subsequent System: Not Availability Impact to the Subsequent System:	m: Low ne None em: None one
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/ABase Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None	A:N
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CWE	CWE-523	
Affected items		Variation
Web Server		1

## SSL/TLS Not Implemented

Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable Integrity Impact to the Vulnerable Syste Availability Impact to the Vulnerable Sy Confidentiality Impact to the Subsequent Integrity Impact to the Subsequent Systems Availability Impact to the Subsequent Systems	tem: Low ystem: None ent System: None stem: None
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C Base Score: 5.4 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None	C:L/I:L/A:N
Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_define Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CWE-319	
Affected items	Variation
Web Server	1

## **(i)** Content Security Policy (CSP) Not Implemented

User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Integrity Impact: None Availability: Not_defined Remediation Level: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Integrity Requirement: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Integrity Requirement: Not_defined Integrity Requirement: Not_defined Complete Integrity Requirement: Not_defined	CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None Availability Impact to the Subsequent System: None Availability Impact to the Subsequent System: None Confidentiality Impact to the Subsequent System: None Availability Impact to the Subsequent System: None Confidentiality Impact System: None Confidentiality	n: None e one m: None ne
Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined  CWE  CWE-1021  Variation	CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None	:N
Affected items Variation	CVSS2	Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined	
	CWE	CWE-1021	
Web Server 1	Affected items		Variation
	Web Server		1

## **(i)** Permissions-Policy header not implemented

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:IN/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None	i: None e one m: None ne
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None	:N
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CWE	CWE-1021	
Affected items		Variation
Web Server		1

#### Alerts details

## Insecure HTTP Usage

Severity	Medium
Reported by module	/target/http_redirections.js

#### Description

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

#### **Impact**

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

#### Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

#### References

HTTP Redirections (https://infosec.mozilla.org/guidelines/web\_security#http-redirections)

#### Affected items

#### **Web Server**

#### Details

#### Request headers

GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip, deflate, br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

Host: 172.23.144.1

Connection: Keep-alive

## **Password transmitted over HTTP**

Severity	Medium
Reported by module	/Crawler/12-Crawler_User_Credentials_Plain_Text.js

#### Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

#### **Impact**

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

#### Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

#### Affected items

#### **Web Server**

#### Details

Forms with credentials sent in clear text:

http://172.23.144.1/dvwa/login.php

```
Form name: <empty>
Form action: login.php
Form method: POST
Password input: password
```

#### Request headers

```
GET /dvwa/login.php HTTP/1.1

Referer: http://172.23.144.1/dvwa/

Cookie: security=impossible; PHPSESSID=umcqg13mq3es622i5913q7o0kv

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

Host: 172.23.144.1

Connection: Keep-alive
```

## SSL/TLS Not Implemented

Severity	Medium
Reported by module	/RPA/no_https.js

#### Description

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

#### **Impact**

Possible information disclosure.

#### Recommendation

The site should send and receive data over a secure (HTTPS) connection.

#### Affected items

#### **Web Server**

Verified vulnerability

Details

#### Request headers

GET /dvwa/ HTTP/1.1

```
D-f----- h----//170 00 144 1/----
```

Referer: http://172.23.144.1/dvwa/

Cookie: security=impossible; PHPSESSID=umcqg13mq3es622i5913q7o0kv

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip, deflate, br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like

Gecko) Chrome/121.0.0.0 Safari/537.36

Host: 172.23.144.1

Connection: Keep-alive

## Ontent Security Policy (CSP) Not Implemented

Severity	Informational
Reported by module	/httpdata/CSP_not_implemented.js

#### Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

#### Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

#### Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

#### References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP) Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

#### Affected items

#### **Web Server**

#### Details

Paths without CSP header:

http://172.23.144.1/dvwa/config/

#### Request headers

GET /dvwa/config/ HTTP/1.1

Referer: http://172.23.144.1/dvwa/

Cookie: security=impossible; PHPSESSID=umcqg13mq3es622i5913q7o0kv

Accept: text/html,application/xhtml+xml,application/xml; g=0.9, \*/\*; g=0.8

Accept-Encoding: gzip, deflate, br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

Host: 172.23.144.1

Connection: Keep-alive

## Open Permissions-Policy header not implemented

Severity	Informational
Reported by module	/httpdata/permissions_policy.js

## Description

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

### **Impact**

#### Recommendation

#### References

<u>Permissions-Policy / Feature-Policy (MDN) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy) Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)</u>

#### Affected items

#### **Web Server**

#### Details

Locations without Permissions-Policy header:

http://172.23.144.1/dvwa/config/

#### Request headers

GET /dvwa/config/ HTTP/1.1

Referer: http://172.23.144.1/dvwa/

Cookie: security=impossible; PHPSESSID=umcqg13mq3es622i5913q7o0kv

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

Host: 172.23.144.1

Connection: Keep-alive

# Scanned items (coverage report)

http://172.23.144.1/